The Founder's Security Checklist

15 checks before you ship your vibe-coded MVP | simonroses.com | Vibe Coding Security Series, Part 8

FIX THESE FIRST:

> Check 4 (secrets already leaked — rotate now)
> Check 9 (any user can see everyone's data)
> Check 1 (no HTTPS = everything interceptable)

THE PERIMETER

- [ ] **1.** Force HTTPS on every page
  `curl -I http://yourapp.com → 301/308 redirect`
- [ ] **2.** Set security headers (score B+ on securityheaders.com)
  `curl -I https://yourapp.com | grep strict-transport`
- [ ] **3.** Close exposed DB ports and admin panels
  `nmap -Pn -p 5432,27017,6379,3306,9200 yourapp.com`

SECRETS

- [ ] **4.** No hardcoded secrets in code or git history
  `gitleaks detect --source . --report-format json`
- [ ] **5.** .env excluded from git, no secrets in Docker layers
  `git ls-files | grep .env → should return nothing`
- [ ] **6.** CORS locked to your own domains only
  `curl -H "Origin: https://evil.com" -I yourapp.com/api`

AUTHENTICATION & ACCESS

- [ ] **7.** Rate limiting on login, signup, and password reset
  `20 rapid requests → should trigger 429 after 5-10`
- [ ] **8.** Every API endpoint checks authentication
  `curl -s yourapp.com/api/notes → 401 Unauthorized`
- [ ] **9.** Users can only access their own data (no IDOR)
  `curl with user A token + user B resource ID → 403`

DATA HANDLING

- [ ] **10.** Server-side input validation on all fields
  `<script>alert(1)</script> → rejected or escaped`
- [ ] **11.** Parameterized queries (no string concatenation)
  `grep -rn "query.*\`.*\${" ./src/ → zero matches`
- [ ] **12.** No tokens or secrets in localStorage
  `DevTools → Application → Local Storage → no auth tokens`

DEPENDENCIES & DEPLOYMENT

- [ ] **13.** Dependencies audited for known vulnerabilities
  `npm audit → zero high/critical findings`
- [ ] **14.** File uploads restricted (type, size, storage)
  `Upload .html/.svg → rejected or not rendered`
- [ ] **15.** Errors don't leak stack traces or internal paths
  `Malformed request → generic error, no stack trace`

ESSENTIAL TOOLS

Secrets:	`gitleaks, trufflehog`
Headers:	`securityheaders.com`
Ports:	`nmap, shodan.io`
Dependencies:	`npm audit, pip-audit, snyk`
CORS:	`curl with Origin header`